PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282974
(43)Date of publication of application : 15.10.1999

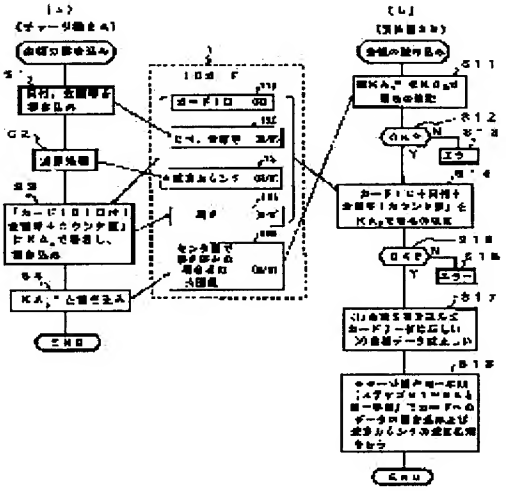
(51)Int.Cl. G06K 17/00
G07F 7/12
G07F 7/08

(21)Application number : 10-086564
(22)Date of filing : 31.03.1998

(71)Applicant : TAMURA ELECTRIC WORKS LTD
(72)Inventor : KOSEKI YOSHINORI

(54) METHOD FOR TRANSFERRING VALUE

(57)Abstract:
PROBLEM TO BE SOLVED: To inexpensively constitute a system and to secure high security by permitting a writing device to write value information in an IC card, execute electronic signing by means of plural specified keys and record it in the card and permitting a reading device to inspect the sign recorded in the card by means of the plural specified keys and transfer value information in accordance with the inspection result.
SOLUTION: When value information is written in the IC card 1, a charge equipment 2A subtracts the value of a subtracting counter 13, electronically signs ID of the card, value information and respective kinds of data of the value in the counter 13 by its own secret key KAs and previously record s a sign open key KAs obtained by previously and electronically signing its own secret key KAs by a common open key KCs in the card 1. In the meantime, a paying equipment 2B inspects the sign open key KApe recorded in the card 1 by the common open key KCs, inspects the sign of electronic sign data recorded in the card 1 by the open key KAp when KApe is correct and transfers value information in accordance with the result.



* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A memory which has a value information field where ID areas where peculiar ID is memorized, and value information are memorized.
An IC card which consists of backward counters.
A writing device which has a common public key common to a system while having a peculiar secret key, and this secret key and a pair of public key, and writes value information in said IC card.
A reader which reads value information which has said common public key while having a peculiar secret key, and this secret key and a pair of public key, and was written in said IC card.
If it is the transport-of-value method provided with the above and said writing device writes value information in an IC card, while subtracting a value of said backward counter, Carry out the electronic signature of each data of a value of ID of an IC card, value information, and a backward counter with an own secret key, and this electronic signature data is recorded on an IC card, And while an own public key records beforehand a signature public key by which the electronic signature was carried out with a common secret key common to a system on an IC card, Said reader verifies a signature of a signature public key of a writing device recorded on an IC card by said common public key, When a verification result is judged to be the right, a signature of electronic signature data recorded on an IC card is verified by a public key of a writing device, and value information is transferred according to the verification result.

[Claim 2]In claim 1, write in said writing device while it writes said value information in an IC card, and it writes in a date at the time, A transport-of-value method while carrying out the electronic signature of the data containing said date with an own secret key and recording on an IC card, wherein said reader verifies a signature of electronic signature data containing said date by a public key of a writing device.
[Claim 3]Claim 1 or claim 2 characterized by comprising the following.
Said writing device performs a message digest operation of data containing a value of ID of an IC card, value information, and a backward counter, While an own secret key performs an electronic signature and that result of an operation is recorded on an IC card, said reader verifies a signature of said electronic signature data recorded on an IC card by a public key of a writing device, and it is this verification result.
ID of an IC card, value information, and a value of a backward counter.

[Claim 4]In which claim of claim 1 thru/or claim 3, said writing device ID of an IC card, Encipher data containing a value of value information and a backward counter with an own secret key, and this encryption data is recorded on an IC card, And while an own public key records beforehand a signature public key enciphered with said common secret key on an IC card, A transport-of-value method decrypting and verifying said encryption data recorded on an IC card when said reader decrypted a signature public key of a writing device recorded on an IC card by said common public key and a decoding result was judged to be the right by a public key of a writing device.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the transport-of-value method of transferring value information.
[0002]
[Description of the Prior Art]As a method of transferring value information, the public-key crypto system using a secret key and a public key as shown in drawing 4 is known. That is, this public-key crypto system performs an electronic signature for the plaintext a which shows value information, for example using secret key K_S. And the electronic signature of this plaintext b with a signature is beforehand notified from the signature side, and the above-mentioned secret key K_S and a pair carry out **** verification for public key K_P. When performing an electronic signature, the plaintext a can be enciphered using secret key K_S, and the plaintext a can also be verified with checking the plaintext a to which the cryptogram was beforehand notified from the signature side and which was decrypted by carrying out **** decryption for public key K_P.
[0003]In the case of such a public-key crypto system, by the signature side, it is the electronic signature which performed the message digest operation (checksum operation) of the plaintext a, and enciphered by secret key K_S to the message digest value, and it specifically sends to the verification side with the plaintext a. On the other hand, in the verification side, if the message digest operation of the plaintext a which received from the signature side is performed, the result of an operation is compared with its decoding result which decrypted the electronic signature received from the signature side by public key K_P and the result of both sides is in agreement, it will judge with the electronic signature being performed correctly.
[0004]There is a method using the protocol called "Card to Card" as shown in drawing 5 as a concrete example of such a public-key crypto system. Here, in drawing 5, the IC card which carries out the electronic signature of the value information which A recorded while value information was recorded, and B are the card readers as a new address which the value information of IC card A transfers. The exclusive computing processors called the co-processor (co-processor) which performs encryption of value information and the check of decoding processing or an electronic signature to IC cardA are built in, The security module which is called SAM which contains the above-mentioned co-processor in the card reader B and which cannot be disassembled is built in, The below-mentioned electronic money which includes value information (amount information) from IC cardA to the card reader B based on the operation by these co-processors and SAM transfers maintaining high security nature.
[0005]By the way, the public key of the IC card issuing center which numerals KC_P shown in drawing 5 does not illustrate, The public key of IC card A, the public key from which public key KA_P was signed to numerals KA_P by secret key KC_S of the center as for numerals $KA_P{}^e$, The secret key of IC card A and numerals KB_P numerals KA_S The public key of the card reader B, Numerals

KB_P^e is the public key from which public key KB_P was signed by secret key KC_S of the center, and public key KC_P is given to IC cardA and the card reader B from the IC card issuing center among each of these keys at the time of issue of IC card A. Public key KA_P^e and KB_P^e are memorized by IC cardA and the card reader B, respectively, and secret key KA_S is further memorized by IC card A.

[0006]If IC card A inputs public key KB_P^e of the card reader B first here when performing transport of value to the card reader B from IC cardA, The right or wrong of a public key KB_P^e signature of the card reader B are checked for the public key KB_P^e using public key KC_P of a card issuing center (Step S21). And it judges whether the signature of the public key KB_P^e is the right (Step S22), if signed correctly, it will shift to Step S24, and it will be in the waiting state of the random number sent from the card reader B. If the signature of public key KB_P^e of the card reader B is not signed correctly, error handling is performed and it ends (Step S23).

[0007]On the other hand, if public key KA_P^e of IC card A is inputted also in the card reader B, the right or wrong of a signature of public key KA_P^e will be checked for the signature of the public key KA_P^e using public key KC_P of a card issuing center (Step S31). And if it judges whether the signature of the public key KA_P^e is the right (Step S32) and is not signed correctly, error handling is performed (Step S33) and processing is ended. If public key KA_P^e of IC card A is signed correctly, while taking out public key KA_P of a decoding result, a random number will be generated, and it will send to IC card A (Step S34), and will be in the waiting state of the electronic money transmitted from after that IC cardA. When a random number is received from the card reader B, in IC cardA Card ID of IC card A, An electronic signature is carried out by own secret key KA_S to each data of the date by which value information was recorded on the card A, the amount of money which shows the value information of the card A, and the received random number (Step S24), and it sends to the card reader B by making it into electronic money.

[0008]In the card reader B, it is verified using public key KA_P (the above-mentioned secret key KA_S and a pair of public key) of IC card A whether the signature of electronic money is the right about the electronic money sent from IC cardA (Step S35). And if electronic money is not signed correctly, while performing error handling (Step S37) and ending processing, When electronic money is signed correctly and the judgment of Step S36 is set to "Y", the amount information decrypted among the electronic money from IC cardA is remitted to a host CPU (Step S38). As a result, in a host CPU, the service based on use of this IC card A is permitted, and the amount information as a result of service provision is subtracted from IC cardA. Thus, the move of the value information to the card reader A is performed from IC cardA.

[0009]

[Problem(s) to be Solved by the Invention]In the transport-of-value system called above-mentioned "Card to Card", since delivery of the key by a public-key crypto system, an electronic signature, and encoding technology are used, there is the feature that the decipherment and forgery by a third party are difficult, therefore can secure high security nature in the case of transport of value. Since the co-processor which performs a key, encryption processing, and electronic signature processing is enclosed with the IC card, decomposition by a third party also has the feature that it is difficult, therefore the decipherment by a third party is very difficult.

[0010]However, in order to perform such public-key-encryption processing, the above-mentioned co-processor which performs encryption, decryption, and an electronic signature check to an IC card needed to be formed, and there was a problem that an IC card became expensive. a co-processor -- even using -- there was a problem that processing time, such as encryption

processing, took a long time. Therefore, an object of this invention is to secure high security nature, while constituting a system cheaply when performing transport of value.
[0011]
[Means for Solving the Problem]If a writing device writes value information in an IC card using an IC card which has a backward counter which will subtract if this invention writes in value information in order to solve such a technical problem, while subtracting a value of a backward counter, Carry out the electronic signature of each data of a value of ID of an IC card, value information, and a backward counter with an own secret key, and this electronic signature data is recorded on an IC card, And while an own public key records beforehand a signature public key by which the electronic signature was carried out with a common secret key common to a system on an IC card, A reader verifies a signature of a signature public key of a writing device recorded on an IC card by a common public key common to a system, It is the method which verifies a signature of electronic signature data recorded on an IC card by a public key of a writing device when a verification result is judged to be the right, and transferred value information according to the verification result. Write in a writing device, when writing value information in an IC card, and it writes in a date at the time, While carrying out the electronic signature of the data containing the date with an own secret key and recording on an IC card, a reader is the method which verified a signature of electronic signature data containing the date by a public key of a writing device. A writing device performs a message digest operation of data containing a value of ID of an IC card, value information, and a backward counter, While recording on an IC card by making into an electronic signature what enciphered that result of an operation with an own secret key, by a public key of a writing device, a reader decodes a signature of electronic signature data recorded on an IC card, and This decoding result, It is the method which compares the message digest result of an operation of data containing a value of ID of an IC card, value information, and a backward counter, and judged right or wrong of an electronic signature, and right or wrong of value information.
[0012]
[Embodiment of the Invention]Hereafter, this invention is explained with reference to drawings. Drawing 1 is a block diagram of the IC card which constitutes the system which applied the transport-of-value method concerning this invention. In the figure, the backward counter 13 as ROM11, the non-volatile RAM 12, and a unique value generator that generates a unique value in the case of dealings of value information is formed in IC card 1. Here, card ID which shows ID of this IC card is stored in card ID areas 11A of ROM11. The signature areas 12A where the data by which the electronic signature was carried out is stored, the public key area 12B where a public key is memorized and a date, the date in which amount information is stored, and the amount-of-money area 12C are established in RAM12.
[0013]Next, the charge machine 2A with which drawing 2 writes in amount information to IC card 1, Or in order to receive offer of service, when IC card 1 is inserted, it is a block diagram showing the composition of payment machine 2B which subtracts the amount of money according to service from the amount information of an insertion card, and both the charge machine 2A and payment machine 2B are the same composition. Thus, this transport-of-value system consists of IC card 1, the charge machine 2A, and a payment machine 2B.
[0014]The charge machine 2A and payment machine 2B consist of SAM21 and CPU25 which are the security modules which cannot be disassembled, IC card interface 26, the memory 27, the key 28, and the display for indication 29, as shown in drawing 2. Here, SAM21 consists of CPU22, the non-volatile RAM 23, and the memory 24, and the amount-of-money data area 23A which memorizes money data, and the encryption key area 23B which memorizes a secret key (encryption key) are established in the non-volatile RAM 23.
[0015]If CPU25 of the charge machine 2A detects insertion of IC card 1 via IC card interface 26, will record amount information on the IC card 1, but. In that case, the money data based on operation of the key 28 or the money data memorized beforehand in the area 23A in the non-volatile RAM 23 of SAM21 is incorporated via CPU22, While writing the money data in the area 12C of the non-volatile RAM 12 of IC card 1 via the interface 26, It reads from clock IC which does not illustrate the time at that time, and writes in the special area of the area 12C as date data, and one

value of the backward counter 13 of IC card 1 is subtracted in that case.
[0016]And card ID in ROM11, the value of the backward counter 13, the date data written in the date of RAM12 and the amount-of-money area 12C, and money data are further read from IC card 1, and it sends to CPU22 of SAM21. The message digest operation of each of these data is performed, it enciphers to the data of the result of an operation with the secret key (encryption key) read from the area 23B of the own non-volatile RAM 23, and CPU22 of SAM21 is taken as an electronic signature. And this signature data is sent to CPU25 and it is made to write in the signature areas 12A of IC card 1. Then, CPU22 in SAM21 sends the public key (public key [finishing / an electronic signature / in the above-mentioned secret key and the secret key of a pair of center apparatus which is not illustrated]) of charge machine 2A itself [which is beforehand memorized by the non-volatile RAM 23] to CPU25, and is made to record it on the public key area 12B of IC card 1.
[0017]In this way, if the card 1 is inserted in payment machine 2B in order for the charge machine 2A to receive various services using IC card 1 on which amount information was recorded, CPU25 of payment machine 2B will read the public key of the public key area 12B of IC card 1 via the interface 26. And the public key whose read charge machine 2A has been signed is sent to CPU22 of SAM21. CPU22 of SAM21 takes out the public key of the charge machine 2A, when the electronic signature of the public key is verified using the public key of the center apparatus which is carrying out hold stores to the non-volatile RAM 23 and the signature of the public key of IC card 1 is judged to be the right. Then, it points to CPU25 and the signature data signed with the secret key of the charge machine 2A is made to read from the signature data area 12A of IC card 1.
[0018]By the secret key of the charge machine 2A, and a pair of above-mentioned public key, CPU22 decodes the signature of the signature data read by CPU25, and And the decoding result, The right or wrong of the signature data of IC card 1 are judged by comparing with the message digest result of an operation about the date data of card ID read from the IC card by CPU25, the value of the backward counter 13, a date, and the amount-of-money area 12C, and money data. Here, when the signature data of IC card 1 is judged to be the right, payment machine 2B subtracts the amount information as a result of service provision from IC card 1 while providing the service based on use of IC card 1. Thus, the move of the value information from the charge machine 2A to payment machine 2B is performed through IC card 1.
[0019]Drawing 3 is a flow chart of the charge machine 2A and payment machine 2B which perform the above operations. Important section operation of this invention is explained according to this flow chart. The public key of the center apparatus which numerals KC_P does not illustrate in drawing 3 probably, The public key of the charge machine 2A, the public key from which public key KA_P was signed to numerals KA_P by secret key KC_S of the center apparatus as for numerals $KA_P{}^e$, Numerals KA_S is a secret key of the charge machine 2A, and public key KC_P of the center is beforehand given to the charge machine 2A and payment machine 2B from the center apparatus. Secret key KA_S and its secret key KA_S, and public key $KA_P{}^e$ signed [a pair of] are memorized by the charge machine 2A.
[0020]Here, when the charge machine 2A records amount information on IC card 1, the date data at that time is written in the area 12C of the non-volatile RAM 12 of IC card 1 with money data (Step S1). And if such money data is written in, subtraction treatment which subtracts one value of the backward counter 13 of IC card 1 automatically will be performed (Step S2). Further And IC card 1 to card ID and the value of the backward counter 13, The date of RAM12, the date data of the amount-of-money area 12C, and money data are read, The message digest operation of each of these data is performed, the electronic signature of that result of an operation is carried out by secret key (encryption key) KA_S memorized in the area 23B of the own non-volatile RAM 23, and this signature data is written in the signature areas 12A of IC card 1 (Step S3). Then, by secret key KC_S of the center apparatus which the charge machine 2A itself does not illustrate, public key (above-mentioned secret key and a pair of public key) $KA_P{}^e$ signed beforehand is recorded on the

public key area 12B of IC card 1 (step S4), and it ends.
[0021]In this way, if the card 1 is inserted in payment machine 2B in order for the charge machine 2A to receive various services using IC card 1 on which amount information was recorded, payment machine 2B will read public key KA_P^e of the public key area 12B of IC card 1 first. And self verifies the right or wrong of a signature of the read public key KA_P^e using public key KC_P of the center apparatus which is carrying out hold stores (Step S11), and it is judged whether the public key KA_P^e is signed correctly.

[0022]When public key KA_P^e of IC card 1 is not signed correctly, perform error handling (Step S13), and end here, but. If public key KA_P^e is signed correctly and the judgment of Step S12 is set to "Y", while taking out and holding public key KA_P of the charge machine 2A, The signature data signed by secret key KA_S of the charge machine 2A is read from the signature data area 12A of IC card 1. By secret key KA_S of the charge machine 2A, and a pair of above-mentioned public key KA_P, decode the signature of the read signature data and And the decoding result, The right or wrong of a signature of signature data are judged by comparing the result of an operation by the message digest operation of the date data of card ID read from the IC card, the counted value of the backward counter 13, a date, and the amount-of-money area 12C, and money data (Step S14).

[0023]When the above-mentioned signature data is not signed correctly, perform error handling (Step S16), and end, but. If signature data is signed correctly and the judgment of Step S15 is set to "Y", payment machine 2B will judge with the money data written in the charge machine 2A being the right amount of money while judging the charge machine 2A which wrote the amount of money in IC card 1 to be the right charge machine 2A. In this case, payment machine 2B subtracts the amount information as a result of service provision from IC card 1, and writes it in in Step S1 of the charge machine 2A - the same procedure as S4 while it provides the service based on use of IC card 1 (Step S18).
[0024]Namely, if the money data of IC card 1 judges with a right thing, payment machine 2B, Subtract the amount information as a result of service provision from the date of IC card 1, and the amount of money of the amount-of-money area 12C like the charge machine 2A, and the balance is written in the area 12C, And while reading in clock IC which does not illustrate the date at that time and recording on the special area of the area 12C, the one backward counter 13 of IC card 1 is subtracted. Further And IC card 1 to card ID and the value of the backward counter 13, Date data and money data are read, the message digest operation of each of these data is performed, and it enciphers by own secret key KB_S to the data of the result of an operation, and writes in the signature areas 12A of IC card 1 by making this into signature data. Then, public key (above-mentioned secret key and a pair of public key) KB_P^e of payment machine 2B itself beforehand signed by secret key KC_S of the center apparatus is recorded on the public key area 12B of IC card 1.
[0025]Thus, value information transfers from the charge machine 2A to payment machine 2B through IC card 1. When payment machine 2B performs data recording as mentioned above to used IC card 1, Even when the IC card 1 is used with a next different payment machine, in the payment machine, like payment machine 2B, verification of a signature of a public key and the signature of data can be verified, and the justification of the amount of money recorded by the justification of payment machine 2B and payment machine 2B can be judged.
[0026]Although Step S3 and S4 of drawing 3 explained the electronic signature of card data, and the electronic signature of the public key of the charge machine 2A, respectively, In this case, these electronic signatures are equivalent to the encryption (it corresponds to Step S3) by the secret key of card data, and the encryption (it corresponds to step S4) by the secret key of the center apparatus of the public key of the charge machine 2A respectively. Although Steps S11 and S14 of drawing 3 explained verification of a signature of the public key of the charge machine 2A,

and verification of the electronic signature of card data, respectively, In this case, verification of these electronic signatures is equivalent to the decryption (it corresponds to Step S11) by the public key of the center apparatus of the public key of the charge machine 2A, and the decryption (it corresponds to Step S14) by the public key of card data respectively.

[0027]Thus, transport of value can be performed, without building an expensive exclusive processor (co-processor) in IC card 1, since value information was transferred from payment machine 2B from the charge machine 2A, and payment machine 2B to other payment machines through IC card 1. Therefore, IC card 1 can be constituted cheaply and the cost of the whole system can be reduced. The backward counter 13 of IC card 1 is certainly subtracted, if the amount of money is written in the card 1, and it cannot write in the value specified arbitrarily. Therefore, when performing transport of value through such a card 1, high security nature comparable as the former can be secured.

[0028]Since CPU22 in each SAM21 of the charge machine 2A and payment machine 2B can be constituted from high-speed one-chip CPU in which high-speed encryption processing and high-speed decoding processing are possible, required encryption and decoding processing can be performed on reservation of high security nature at high speed in the case of transport of value. If the backward counter 13 of IC card 1 is used also for attestation of arbitrary messages, for example, without using only for attestation of the amount of money, it will become possible to use IC card 1 as a multiple use card. Whenever the backward counter 13 is good also as a forward counter and writes the amount of money in IC card 1 in short, it should just be a means which changes automatic only the value to a best unique value.

[0029]

[Effect of the Invention]While subtracting the value of a backward counter using the IC card which has a backward counter which will subtract if value information is written in according to this invention if a writing device writes value information in an IC card as explained above, Carry out the electronic signature of each data of the value of ID of an IC card, value information, and a backward counter with an own secret key, and this electronic signature data is recorded on an IC card, And while an own public key records beforehand the signature public key by which the electronic signature was carried out with the common secret key common to a system on an IC card, A reader verifies the signature of the signature public key of the writing device recorded on the IC card by a common public key common to a system, Since the signature of the electronic signature data recorded on the IC card is verified by the public key of a writing device and value information was transferred according to the verification result when a verification result was judged to be the right, Transport of value can be performed without building an expensive exclusive processor (co-processor) in an IC card. Therefore, while being able to constitute an IC card cheaply and being able to reduce the cost of the whole system, high security nature is securable in the case of transport of value. Write in a writing device, when writing value information in an IC card, and it writes in the date at the time, While carrying out the electronic signature of the data containing the date with an own secret key and recording on an IC card, since the reader verified the signature of the electronic signature data containing the date by the public key of the writing device, its security nature in the case of transport of value improves further. A writing device performs the message digest operation of the data containing the value of ID of an IC card, value information, and a backward counter, While an own secret key performs an electronic signature and that result of an operation is recorded on an IC card, by the public key of a writing device, verify a reader and the signature of the electronic signature data recorded on the IC card This verification result, Since the message digest result of an operation of the data containing the value of ID of an IC card, value information, and a backward counter is compared and the right or wrong of an electronic signature and the right or wrong of value information were judged, in the case of transport of value, security nature can be improved similarly.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－282974

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｄ
			Ｌ
			Ｒ
			Ｔ
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｃ

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平10－86564

(22)出願日　平成10年(1998)３月31日

(71)出願人　000003632
株式会社田村電機製作所
東京都目黒区下目黒２丁目２番３号

(72)発明者　小関　吉則
東京都目黒区下目黒二丁目２番３号　株式会社田村電機製作所内

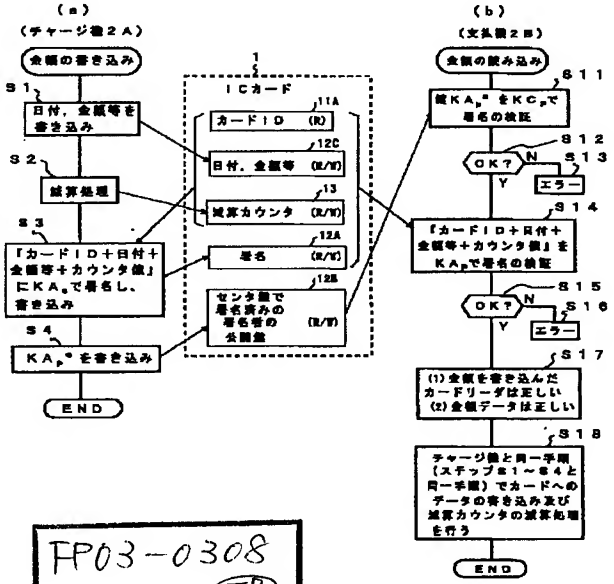
(74)代理人　弁理士　山川　政樹

(54)【発明の名称】　価値移転方法

(57)【要約】

【課題】　価値移転を行う際に、システムを安価に構成するとともにシステムの高セキュリティ性を確保する。

【解決手段】　ＩＣカード１を媒介としてチャージ機２Ａから支払機２Ｂへ価値情報を移転するものであり、チャージ機はＩＣカードに価値情報を書き込むとＩＣカードの減算カウンタ１３を減算するとともに、ＩＣカードのＩＤ、価値情報及び減算カウンタの値を含む各データを自身の秘密鍵KA_Sで電子署名しこの電子署名データをＩＣカードに記録し、かつ自身の公開鍵KA_Pをセンタ装置の秘密鍵KC_Sで電子署名しこの署名公開鍵KA_{Pe}をＩＣカードに記録する一方、支払機２Ｂは ＩＣカードに記録された署名公開鍵KA_{Pe}の署名をセンタ装置の公開鍵KC_Pで検証し、検証結果が正しい場合はＩＣカードに記録された電子署名データの署名を公開鍵KA_Pで検証しその検証結果に応じて価値情報を移転する。



FP03-0308
JP
'08. 5. 07
OA

【特許請求の範囲】

【請求項１】　固有のＩＤが記憶されるＩＤ領域及び価値情報が記憶される価値情報領域を有するメモリと、減算カウンタとからなるＩＣカードと、固有の秘密鍵及びこの秘密鍵と対の公開鍵を有するとともにシステム共通の共通公開鍵を有し、前記ＩＣカードに価値情報を書き込む書き込み装置と、固有の秘密鍵及びこの秘密鍵と対の公開鍵を有するとともに前記共通公開鍵を有し、前記ＩＣカードに書き込まれた価値情報の読み取りを行う読み取り装置とを備えたシステムにおける価値情報の移転方法であって、

前記書き込み装置はＩＣカードに価値情報を書き込むと前記減算カウンタの値を減算するとともに、ＩＣカードのＩＤ、価値情報及び減算カウンタの値の各データを自身の秘密鍵で電子署名しこの電子署名データをＩＣカードに記録し、かつ予め自身の公開鍵がシステム共通の共通秘密鍵で電子署名された署名公開鍵をＩＣカードに記録する一方、

前記読み取り装置はＩＣカードに記録された書き込み装置の署名公開鍵の署名を前記共通公開鍵で検証し、検証結果が正しいと判定された場合はＩＣカードに記録された電子署名データの署名を書き込み装置の公開鍵で検証し、その検証結果に応じて価値情報を移転することを特徴とする価値移転方法。

【請求項２】　請求項１において、

前記書き込み装置はＩＣカードに前記価値情報を書き込むとともに書き込み時点の日付を書き込み、前記日付を含むデータを自身の秘密鍵で電子署名してＩＣカードに記録する一方、前記読み取り装置は前記日付を含む電子署名データの署名を書き込み装置の公開鍵で検証することを特徴とする価値移転方法。

【請求項３】　請求項１または請求項２において、

前記書き込み装置はＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算を行い、その演算結果を自身の秘密鍵で電子署名を行いＩＣカードに記録する一方、前記読み取り装置はＩＣカードに記録された前記電子署名データの署名を書き込み装置の公開鍵で検証し、この検証結果と、ＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算結果とを比較して電子署名の正否及び価値情報の正否を判定することを特徴とする価値移転方法。

【請求項４】　請求項１ないし請求項３の何れかの請求項において、

前記書き込み装置はＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータを自身の秘密鍵で暗号化してこの暗号化データをＩＣカードに記録し、かつ予め自身の公開鍵が前記共通秘密鍵で暗号化された署名公開鍵をＩＣカードに記録する一方、

前記読み取り装置はＩＣカードに記録された書き込み装置の署名公開鍵を前記共通公開鍵で復号化し、復号結果が正しいと判定された場合はＩＣカードに記録された前記暗号化データを書き込み装置の公開鍵で復号化し検証することを特徴とする価値移転方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、価値情報を移転する価値移転方法に関する。

【０００２】

【従来の技術】価値情報を移転する方法として、図４に示すような、秘密鍵及び公開鍵を用いた公開鍵暗号方式が知られている。即ち、この公開鍵暗号方式は、例えば価値情報を示す平文ａを秘密鍵K_S を用いて電子署名を行う。そして、この署名付き平文ｂの電子署名を署名側から予め通知され上記秘密鍵K_S と対の公開鍵K_P 用いて検証するものである。また、電子署名を行う場合、平文ａを秘密鍵K_S を用いて暗号化し、その暗号文を署名側から予め通知された公開鍵K_P 用いて復号化し、復号化された平文ａをチェックすることで平文ａの検証を行うこともできる。

【０００３】なお、こうした公開鍵暗号方式の場合、具体的には署名側では平文ａのメッセージダイジェスト演算（チェックサム演算）を行い、そのメッセージダイジェスト値に秘密鍵K_S で暗号化を行ったものが電子署名で、平文ａとともに検証側へ送る。一方、検証側では署名側から受信した平文ａのメッセージダイジェスト演算を行いその演算結果と、署名側から受信した電子署名を公開鍵K_P により復号化したその復号結果とを比較し、双方の結果が一致するとその電子署名は正しく行われていると判定する。

【０００４】このような公開鍵暗号方式の具体的な例として、図５に示すような、「Ｃａｒｄ　ｔｏ　Ｃａｒｄ」と呼ばれるプロトコルを用いた方式がある。ここで、図５において、Ａは価値情報が記録されるとともに記録した価値情報を電子署名するＩＣカード、ＢはＩＣカードＡの価値情報が移転される移転先としてのカードリーダである。なお、ＩＣカードＡには、価値情報の暗号化，復号化処理や電子署名のチェックを行うコプロセッサ（ｃｏ－ｐｒｏｃｅｓｓｏｒ）と呼ばれる専用演算プロセッサが内蔵され、カードリーダＢにも上記コプロセッサを含むＳＡＭと呼ばれる分解不可能なセキュリティモジュールが内蔵され、これらのコプロセッサ及びＳＡＭによる演算に基づきＩＣカードＡからカードリーダＢへ価値情報（金額情報）を含む後述の電子マネーが高セキュリティ性を維持しながら移転される。

【０００５】ところで、図５に示されている符号K_{CP} は図示しないＩＣカード発行センタの公開鍵、符号K_{AP} はＩＣカードＡの公開鍵、符号K_{AP^e}は公開鍵K_{AP} がセンタの秘密鍵K_{CS} で署名された公開鍵、符号K_{AS} はＩＣカードＡの秘密鍵、符号K_{BP} はカードリーダ

Bの公開鍵、符号K_{BP^e}は公開鍵K_{BP}がセンタの秘密鍵K_{CS}で署名された公開鍵であり、これらの各鍵のうち、公開鍵K_{CP}はＩＣカードＡの発行時にＩＣカード発行センタからＩＣカードＡ及びカードリーダＢに与えられている。また、公開鍵K_{AP^e}，K_{BP^e}はそれぞれＩＣカードＡ及びカードリーダＢに記憶され、さらに秘密鍵K_{AS}はＩＣカードＡに記憶されている。

【０００６】ここで、ＩＣカードＡからカードリーダＢへの価値移転を行う場合、まずＩＣカードＡはカードリーダＢの公開鍵K_{BP^e}を入力すると、その公開鍵K_{BP^e}をカード発行センタの公開鍵K_{CP}を使ってカードリーダＢの公開鍵K_{BP^e}署名の正否をチェックする（ステップＳ２１）。そしてその公開鍵K_{BP^e}の署名が正しいか否かを判断し（ステップＳ２２）、正しく署名されていればステップＳ２４へ移行し、カードリーダＢから送られる乱数の待機状態となる。なお、カードリーダＢの公開鍵K_{BP^e}の署名が正しく署名されていなければ、エラー処理を行って（ステップＳ２３）終了する。

【０００７】一方、カードリーダＢにおいてもＩＣカードＡの公開鍵K_{AP^e}を入力すると、その公開鍵K_{AP^e}の署名をカード発行センタの公開鍵K_{CP}を使って公開鍵K_{AP^e}の署名の正否をチェックする（ステップＳ３１）。そしてその公開鍵K_{AP^e}の署名が正しいか否かを判断し（ステップＳ３２）、正しく署名されていなければ、エラー処理を行い（ステップＳ３３）処理を終了する。また、ＩＣカードＡの公開鍵K_{AP^e}の署名が正しく行われていれば復号結果の公開鍵K_{AP}を取り出すとともに、乱数を発生してＩＣカードＡへ送り（ステップＳ３４）、その後ＩＣカードＡから送信される電子マネーの待機状態となる。ＩＣカードＡでは、カードリーダＢから乱数を受け取ると、ＩＣカードＡのカードＩＤ、カードＡに価値情報が記録された日付、カードＡの価値情報を示す金額、及び受け取った乱数の各データに対し自身の秘密鍵K_{AS}で電子署名し（ステップＳ２４）、それを電子マネーとしてカードリーダＢへ送る。

【０００８】カードリーダＢでは、ＩＣカードＡから送られてきた電子マネーについてＩＣカードＡの公開鍵K_{AP}（上記秘密鍵K_{AS}と対の公開鍵）を用いて電子マネーの署名が正しいか否かを検証する（ステップＳ３５）。そして電子マネーが正しく署名されていなければエラー処理を行い（ステップＳ３７）、処理を終了するとともに、電子マネーが正しく署名されステップＳ３６の判定が「Ｙ」となる場合は、ＩＣカードＡからの電子マネーのうち、復号化された金額情報を上位ＣＰＵへ送る（ステップＳ３８）。この結果、上位ＣＰＵではこのＩＣカードＡの使用に基づくサービスを許容し、サービス提供の結果の金額情報がＩＣカードＡから減じられる。このようにしてＩＣカードＡからカードリーダＡへの価値情報の移転が行われる。

【０００９】

【発明が解決しようとする課題】上記した「Ｃａｒｄ ｔｏ Ｃａｒｄ」と呼ばれる価値移転システムでは、公開鍵暗号方式による鍵の受け渡し、電子署名及び暗号技術を利用しているため、第三者による解読や偽造が難しく、したがって価値移転の際に高セキュリティ性を確保できるという特徴がある。また、ＩＣカードには鍵、暗号化処理及び電子署名処理を行うコプロセッサを封入しているため第三者による分解が困難であり、したがって第三者による解読が極めて困難であるという特徴も有している。

【００１０】しかしながら、こうした公開鍵暗号処理を実行するためには、ＩＣカードに、暗号化，復号化及び電子署名チェックを行う上述のコプロセッサを設ける必要があり、ＩＣカードが高価になるという問題があった。また、コプロセッサを使ってさえも、暗号化処理などの処理時間に長時間を要するという問題があった。したがって本発明は、価値移転を行う場合、システムを安価に構成するとともに高セキュリティ性を確保することを目的とする。

【００１１】

【課題を解決するための手段】このような課題を解決するために本発明は、価値情報を書き込むと減算を行う減算カウンタを有するＩＣカードを用い、書き込み装置はＩＣカードに価値情報を書き込むと減算カウンタの値を減算するとともに、ＩＣカードのＩＤ、価値情報及び減算カウンタの値の各データを自身の秘密鍵で電子署名しこの電子署名データをＩＣカードに記録し、かつ予め自身の公開鍵がシステム共通の共通秘密鍵で電子署名された署名公開鍵をＩＣカードに記録する一方、読み取り装置はＩＣカードに記録された書き込み装置の署名公開鍵の署名をシステム共通の共通公開鍵で検証し、検証結果が正しいと判定された場合はＩＣカードに記録された電子署名データの署名を書き込み装置の公開鍵で検証し、その検証結果に応じて価値情報を移転するようにした方法である。また、書き込み装置はＩＣカードに価値情報を書き込むときに書き込み時点の日付を書き込み、日付を含むデータを自身の秘密鍵で電子署名してＩＣカードに記録する一方、読み取り装置は日付を含む電子署名データの署名を書き込み装置の公開鍵で検証するようにした方法である。また、書き込み装置はＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算を行い、その演算結果を自身の秘密鍵で暗号化したものを電子署名としてＩＣカードに記録する一方、読み取り装置はＩＣカードに記録された電子署名データの署名を書き込み装置の公開鍵で復号し、この復号結果と、ＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算結果とを比較して電子署名の正否及び価値情報の正否を判定するようにした方法である。

【００１２】

【発明の実施の形態】以下、本発明について図面を参照して説明する。図１は本発明に係る価値移転方法を適用したシステムを構成するＩＣカードのブロック図である。同図において、ＩＣカード１にはＲＯＭ１１、不揮発性ＲＡＭ１２、及び価値情報の取引の際にユニークな値を発生するユニーク値発生器としての減算カウンタ１３が設けられている。ここで、ＲＯＭ１１のカードＩＤエリア１１Ａには本ＩＣカードのＩＤを示すカードＩＤが格納される。また、ＲＡＭ１２には、電子署名されたデータが格納される署名エリア１２Ａ、公開鍵が記憶される公開鍵エリア１２Ｂ、及び日付，金額情報が格納される日付，金額エリア１２Ｃが設けられている。

【００１３】次に図２は、ＩＣカード１に対して金額情報を書き込むチャージ機２Ａ、または、サービスの提供を受けるためにＩＣカード１が挿入されたとき挿入カードの金額情報からサービスに応じた金額を減じる支払機２Ｂの構成を示すブロック図であり、チャージ機２Ａ及び支払機２Ｂはともに同様の構成である。このように本価値移転システムは、ＩＣカード１と、チャージ機２Ａと、支払機２Ｂとからなる。

【００１４】チャージ機２Ａ及び支払機２Ｂは、図２に示すように、分解不可能なセキュリティモジュールであるＳＡＭ２１と、ＣＰＵ２５と、ＩＣカードインタフェース２６と、メモリ２７と、キー２８と、表示器２９とからなる。ここで、ＳＡＭ２１は、ＣＰＵ２２と、不揮発性ＲＡＭ２３と、メモリ２４とからなり、不揮発性ＲＡＭ２３には、金額データを記憶する金額データエリア２３Ａと、秘密鍵（暗号鍵）を記憶する暗号鍵エリア２３Ｂとが設けられている。

【００１５】チャージ機２ＡのＣＰＵ２５はＩＣカードインタフェース２６を介してＩＣカード１の挿入を検出すると、そのＩＣカード１に金額情報を記録するが、その場合、キー２８の操作に基づく金額データ、または予めＳＡＭ２１の不揮発性ＲＡＭ２３内のエリア２３Ａに記憶されている金額データをＣＰＵ２２を介して取り込み、その金額データをインタフェース２６を介しＩＣカード１の不揮発性ＲＡＭ１２のエリア１２Ｃに書き込むとともに、そのときの日時を図示しない時計ＩＣから読み込んで、日付データとして同エリア１２Ｃの別途エリアに書き込み、かつその際にはＩＣカード１の減算カウンタ１３の値を１つ減算する。

【００１６】そして、さらにＩＣカード１から、ＲＯＭ１１内のカードＩＤと、減算カウンタ１３の値と、ＲＡＭ１２の日付，金額エリア１２Ｃに書き込まれた日付データと、金額データとを読み出してＳＡＭ２１のＣＰＵ２２に送る。ＳＡＭ２１のＣＰＵ２２は、これらの各データのメッセージダイジェスト演算を行い、その演算結果のデータに対し、自身の不揮発性ＲＡＭ２３のエリア２３Ｂから読み出した秘密鍵（暗号鍵）で暗号化し電子署名とする。そして、この署名データをＣＰＵ２５に送ってＩＣカード１の署名エリア１２Ａに書き込ませる。続いて、ＳＡＭ２１内のＣＰＵ２２は、不揮発性ＲＡＭ２３に予め記憶されているチャージ機２Ａ自身の公開鍵（上記秘密鍵と対の図示しないセンタ装置の秘密鍵で電子署名済みの公開鍵）をＣＰＵ２５に送ってＩＣカード１の公開鍵エリア１２Ｂに記録させる。

【００１７】こうしてチャージ機２Ａで金額情報が記録されたＩＣカード１を用いて種々のサービスを受けるためにそのカード１が支払機２Ｂに挿入されると、支払機２ＢのＣＰＵ２５は、インタフェース２６を介してＩＣカード１の公開鍵エリア１２Ｂの公開鍵を読み取る。そして読み取ったチャージ機２Ａの署名済みの公開鍵をＳＡＭ２１のＣＰＵ２２へ送る。ＳＡＭ２１のＣＰＵ２２はその公開鍵の電子署名を、不揮発性ＲＡＭ２３に記憶保持しているセンタ装置の公開鍵を用いて検証し、ＩＣカード１の公開鍵の署名が正しいと判定される場合は、チャージ機２Ａの公開鍵を取り出す。その後、ＣＰＵ２５に指示してＩＣカード１の署名データエリア１２Ａから、チャージ機２Ａの秘密鍵で署名されている署名データを読み出させる。

【００１８】そしてＣＰＵ２２はＣＰＵ２５により読み出された署名データの署名を、チャージ機２Ａの秘密鍵と対の上記公開鍵で復号し、その復号結果と、ＣＰＵ２５によりＩＣカードから読み出されたカードＩＤ、減算カウンタ１３の値、日付，金額エリア１２Ｃの日付データ、及び金額データについてのメッセージダイジェスト演算結果と比較することにより、ＩＣカード１の署名データの正否を判断する。ここで、ＩＣカード１の署名データが正しいと判断される場合は、支払機２ＢはＩＣカード１の使用に基づくサービスを提供するとともに、サービス提供の結果の金額情報をＩＣカード１から減じる。このようにして、ＩＣカード１を媒介としてチャージ機２Ａから支払機２Ｂへの価値情報の移転が行われる。

【００１９】図３は以上のような動作を行うチャージ機２Ａ及び支払機２Ｂのフローチャートである。このフローチャートにしたがって本発明の要部動作を説明する。まず図３において、符号K_{CP}は図示しないセンタ装置の公開鍵、符号K_{AP}はチャージ機２Ａの公開鍵、符号K_{AP}^{e}は公開鍵K_{AP}がセンタ装置の秘密鍵K_{CS}で署名された公開鍵、符号K_{AS}はチャージ機２Ａの秘密鍵であり、センタの公開鍵K_{CP}は予めセンタ装置からチャージ機２Ａ及び支払機２Ｂに与えられている。また、秘密鍵K_{AS}及びその秘密鍵K_{AS}と対の署名済みの公開鍵K_{AP}^{e}はチャージ機２Ａに記憶されている。

【００２０】ここで、チャージ機２ＡがＩＣカード１に金額情報を記録する場合は、ＩＣカード１の不揮発性ＲＡＭ１２のエリア１２Ｃに金額データとともに、そのときの日付データを書き込む（ステップＳ１）。そして、こうした金額データを書き込むと自動的にＩＣカード１

の減算カウンタ１３の値を１つ減算する減算処理を行う（ステップＳ２）。そしてさらに、ＩＣカード１から、カードＩＤと、減算カウンタ１３の値と、ＲＡＭ１２の日付，金額エリア１２Ｃの日付データと、金額データとを読み出し、これらの各データのメッセージダイジェスト演算を行いその演算結果を、自身の不揮発性ＲＡＭ２３のエリア２３Ｂに記憶されている秘密鍵（暗号鍵）K_{AS} で電子署名し、この署名データをＩＣカード１の署名エリア１２Ａに書き込む（ステップＳ３）。続いて、チャージ機２Ａ自身の、図示しないセンタ装置の秘密鍵 K_{CS} で予め署名された公開鍵（上記秘密鍵と対の公開鍵）K_{APe} をＩＣカード１の公開鍵エリア１２Ｂに記録（ステップＳ４）して終了する。

【００２１】こうしてチャージ機２Ａで金額情報が記録されたＩＣカード１を使用して種々のサービスを受けるためにそのカード１が支払機２Ｂに挿入されると、支払機２Ｂは、まずＩＣカード１の公開鍵エリア１２Ｂの公開鍵 K_{APe} を読み取る。そして読み取ったその公開鍵 K_{APe} の署名の正否を、自身が記憶保持しているセンタ装置の公開鍵 K_{CP} を用いて検証し（ステップＳ１１）、その公開鍵 K_{APe} が正しく署名されているか否かを判断する。

【００２２】ここで、ＩＣカード１の公開鍵 K_{APe} が正しく署名されていない場合はエラー処理（ステップＳ１３）を行って終了するが、公開鍵 K_{APe} が正しく署名されステップＳ１２の判定が「Ｙ」となると、チャージ機２Ａの公開鍵 K_{AP} を取り出して保持するとともに、ＩＣカード１の署名データエリア１２Ａから、チャージ機２Ａの秘密鍵 K_{AS} で署名された署名データを読み出す。そして読み出した署名データの署名を、チャージ機２Ａの秘密鍵 K_{AS} と対の上記公開鍵 K_{AP} で復号し、その復号結果と、ＩＣカードから読み出したカードＩＤ、減算カウンタ１３のカウント値、日付，金額エリア１２Ｃの日付データ、及び金額データのメッセージダイジェスト演算による演算結果とを比較することにより、署名データの署名の正否を判断する（ステップＳ１４）。

【００２３】上記署名データが正しく署名されていない場合は、エラー処理（ステップＳ１６）を行って終了するが、署名データが正しく署名されステップＳ１５の判定が「Ｙ」となると、支払機２Ｂは、ＩＣカード１に金額を書き込んだチャージ機２Ａを正しいチャージ機２Ａと判定するとともに、そのチャージ機２Ａに書き込まれた金額データも正しい金額であると判定する。この場合、支払機２Ｂは、ＩＣカード１の使用に基づくサービスを提供するとともに、サービス提供の結果の金額情報をＩＣカード１から減じ、チャージ機２Ａのステップ１～Ｓ４と同様な手順で書き込む（ステップＳ１８）。

【００２４】即ち、支払機２Ｂは、ＩＣカード１の金額データが正しいものと判定すると、サービス提供の結果の金額情報をチャージ機２Ａと同様、ＩＣカード１の日付，金額エリア１２Ｃの金額から減じて残額をそのエリア１２Ｃに書き込み、かつその時の日付を図示しない時計ＩＣから読み取ってエリア１２Ｃの別途エリアに記録するとともに、ＩＣカード１の減算カウンタ１３を１つ減算する。そしてさらに、ＩＣカード１から、カードＩＤと、減算カウンタ１３の値と、日付データと、金額データとを読み出し、これらの各データのメッセージダイジェスト演算を行い、その演算結果のデータに自身の秘密鍵 K_{BS} で暗号化し、これを署名データとしてＩＣカード１の署名エリア１２Ａに書き込む。続いて、支払機２Ｂ自身の、予めセンタ装置の秘密鍵 K_{CS} で署名された公開鍵（上記秘密鍵と対の公開鍵）K_{BPe} をＩＣカード１の公開鍵エリア１２Ｂに記録する。

【００２５】このようにして、ＩＣカード１を媒介としてチャージ機２Ａから支払機２Ｂへ価値情報が移転される。なお、使用されたＩＣカード１に対し支払機２Ｂが上記のようにデータ記録を行うことにより、そのＩＣカード１が次に異なる支払機で使用された場合でも、その支払機では支払機２Ｂと同様、公開鍵の署名の検証やデータの署名の検証を行い、支払機２Ｂの正当性及び支払機２Ｂにより記録された金額の正当性を判定することができる。

【００２６】なお、図３のステップＳ３及びＳ４では、それぞれカードデータの電子署名及びチャージ機２Ａの公開鍵の電子署名について説明したが、この場合これらの電子署名は、それぞれカードデータの秘密鍵による暗号化（ステップＳ３に対応）及びチャージ機２Ａの公開鍵のセンタ装置の秘密鍵による暗号化（ステップＳ４に対応）と同等である。また、図３のステップＳ１１及びＳ１４では、それぞれチャージ機２Ａの公開鍵の署名の検証及びカードデータの電子署名の検証について説明したが、この場合これら電子署名の検証は、それぞれチャージ機２Ａの公開鍵のセンタ装置の公開鍵による復号化（ステップＳ１１に対応）及びカードデータの公開鍵による復号化（ステップＳ１４に対応）と同等である。

【００２７】このようにＩＣカード１を媒介としてチャージ機２Ａから支払機２Ｂ、支払機２Ｂから他の支払機へと価値情報を移転するようにしたので、ＩＣカード１に高価な専用プロセッサ（コプロセッサ）を内蔵することなく、価値移転を行うことができる。したがってＩＣカード１を安価に構成することができ、システム全体のコストを低減することができる。また、ＩＣカード１の減算カウンタ１３はカード１に金額を書き込むと必ず減算されるものであり、任意に指定された値を書き込むことができない。したがって、こうしたカード１を媒介として価値移転を行う場合、従来と同程度の高セキュリティ性を確保できる。

【００２８】また、チャージ機２Ａ及び支払機２Ｂの各ＳＡＭ２１内のＣＰＵ２２を、高速暗号化処理及び高速

復号化処理可能な高速ワンチップＣＰＵで構成できるため、価値移転の際に高セキュリティ性の確保上必要な暗号化及び復号化処理を高速で行うことができる。また、ＩＣカード１の減算カウンタ１３を、金額の認証だけに用いずに、例えば任意のメッセージの認証にも用いるようにすれば、ＩＣカード１を多目的カードとして利用することが可能になる。なお、減算カウンタ１３は加算カウンタとしても良く、要はＩＣカード１に金額を書き込む毎にその値が自動的に唯一無二のユニークな値に変わるような手段であれば良い。

【００２９】

【発明の効果】以上説明したように本発明によれば、価値情報を書き込むと減算を行う減算カウンタを有するＩＣカードを用い、書き込み装置はＩＣカードに価値情報を書き込むと減算カウンタの値を減算するとともに、ＩＣカードのＩＤ、価値情報及び減算カウンタの値の各データを自身の秘密鍵で電子署名しこの電子署名データをＩＣカードに記録し、かつ予め自身の公開鍵がシステム共通の共通秘密鍵で電子署名された署名公開鍵をＩＣカードに記録する一方、読み取り装置はＩＣカードに記録された書き込み装置の署名公開鍵の署名をシステム共通の共通公開鍵で検証し、検証結果が正しいと判定された場合はＩＣカードに記録された電子署名データの署名を書き込み装置の公開鍵で検証し、その検証結果に応じて価値情報を移転するようにしたので、ＩＣカードに高価な専用プロセッサ（コプロセッサ）を内蔵することなく、価値移転を行うことができる。したがってＩＣカードを安価に構成することができ、システム全体のコストを低減することができるとともに、価値移転の際に高セキュリティ性を確保できる。また、書き込み装置はＩＣカードに価値情報を書き込むときに書き込み時点の日付を書き込み、日付を含むデータを自身の秘密鍵で電子署名してＩＣカードに記録する一方、読み取り装置は日付を含む電子署名データの署名を書き込み装置の公開鍵で検証するようにしたので、価値移転の際のセキュリティ性がさらに向上する。また、書き込み装置はＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算を行い、その演算結果を自身の秘密鍵で電子署名を行いＩＣカードに記録する一方、読み取り装置はＩＣカードに記録された電子署名データの署名を書き込み装置の公開鍵で検証し、この検証結果と、ＩＣカードのＩＤ、価値情報及び減算カウンタの値を含むデータのメッセージダイジェスト演算結果とを比較して電子署名の正否及び価値情報の正否を判定するようにしたので、価値移転の際には同様にセキュリティ性を向上できる。

【図面の簡単な説明】

【図１】　本発明を適用したＩＣカードの構成を示すブロック図である。

【図２】　ＩＣカードに対して価値情報を記録するチャージ機及びＩＣカードの価値情報を読み出す支払機の構成を示すブロック図である。

【図３】　本発明の要部動作を示すフローチャートである。

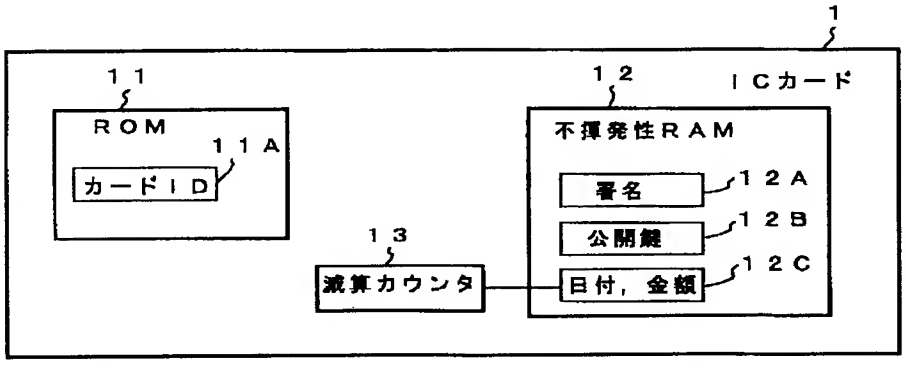
【図４】　公開鍵暗号方式を適用した電子署名及びその電子署名の検証を説明する説明図である。

【図５】　公開鍵暗号方式を用いた従来の価値移転動作を示すフローチャートである。

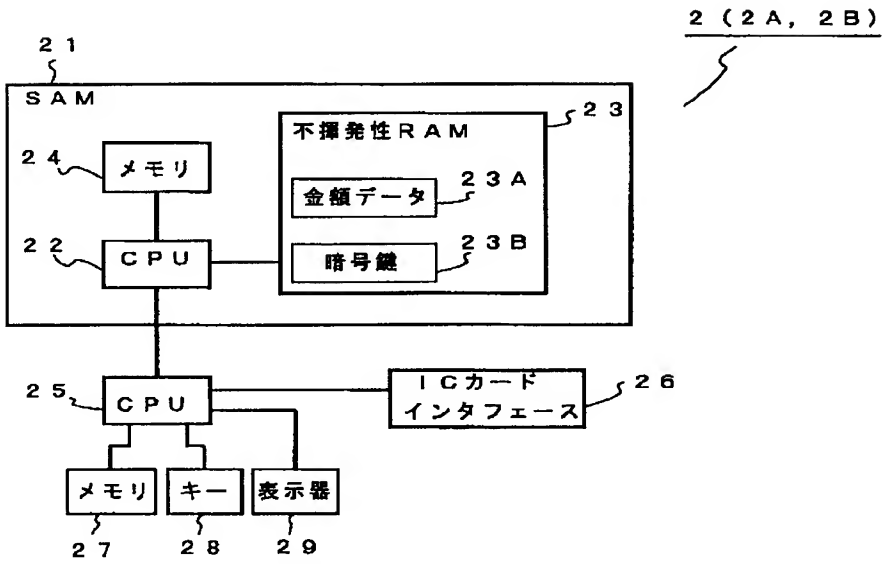
【符号の説明】

１…ＩＣカード、２Ａ…チャージ機、２Ｂ…支払機、１１…ＲＯＭ、１１Ａ…カードＩＤエリア、１２，２３…不揮発性ＲＡＭ、１２Ａ…署名データエリア、１２Ｂ…公開鍵エリア、１２Ｃ…日付，金額エリア、１３…減算カウンタ、２１…ＳＡＭ、２２，２５…ＣＰＵ、２３Ｂ…暗号鍵エリア、２６…ＩＣカードイタフェース。

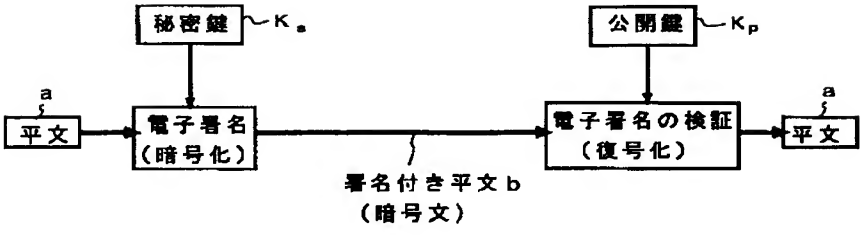
【図１】



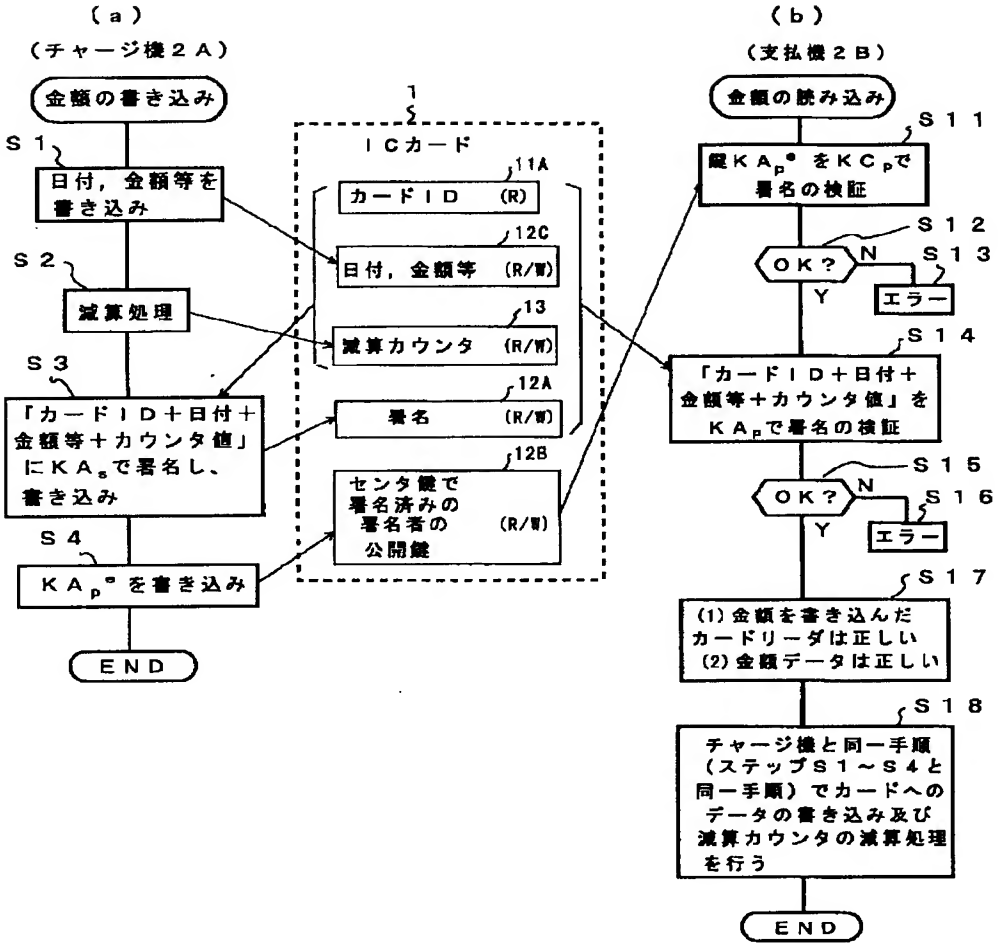
【図２】


２（２Ａ，２Ｂ）
２１
ＳＡＭ
２３
不揮発性ＲＡＭ
２４
メモリ
２３Ａ
金額データ
２２
ＣＰＵ
２３Ｂ
暗号鍵
２５
ＣＰＵ
ＩＣカード
インタフェース
２６
メモリ
キー
表示器
２７
２８
２９

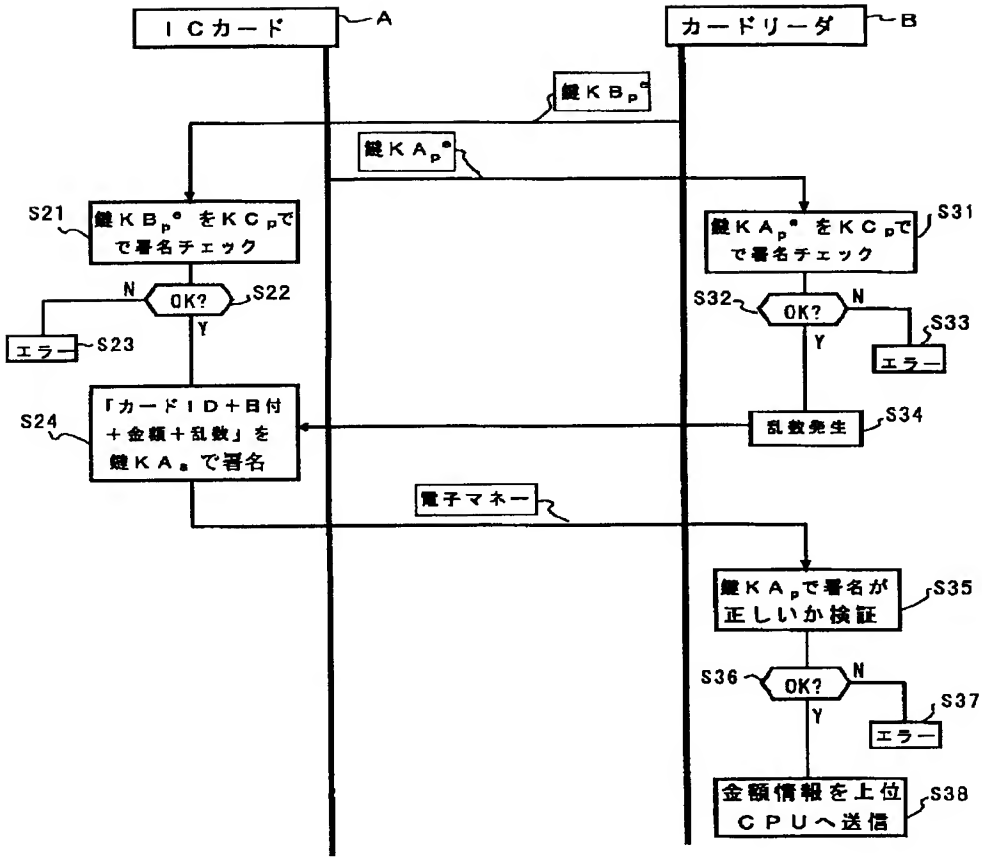
【図４】


秘密鍵
K_s
公開鍵
K_p
a
平文
電子署名
（暗号化）
電子署名の検証
（復号化）
a
平文
署名付き平文ｂ
（暗号文）

【図３】


（ａ）
（チャージ機２Ａ）
金額の書き込み
Ｓ１
日付，金額等を書き込み
Ｓ２
減算処理
Ｓ３
「カードＩＤ＋日付＋金額等＋カウンタ値」にＫＡｓで署名し、書き込み
Ｓ４
ＫＡｐ’を書き込み
ＥＮＤ
１
ＩＣカード
11A
カードＩＤ (R)
12C
日付，金額等 (R/W)
13
減算カウンタ (R/W)
12A
署名 (R/W)
12B
センタ鍵で署名済みの署名者の公開鍵 (R/W)
（ｂ）
（支払機２Ｂ）
金額の読み込み
Ｓ１１
鍵ＫＡｐ’をＫＣｐで署名の検証
Ｓ１２
ＯＫ？
N
Ｓ１３
エラー
Y
Ｓ１４
「カードＩＤ＋日付＋金額等＋カウンタ値」をＫＡｐで署名の検証
Ｓ１５
ＯＫ？
N
Ｓ１６
エラー
Y
Ｓ１７
(1)金額を書き込んだカードリーダは正しい
(2)金額データは正しい
Ｓ１８
チャージ機と同一手順（ステップＳ１～Ｓ４と同一手順）でカードへのデータの書き込み及び減算カウンタの減算処理を行う
ＥＮＤ

【図５】



フロントページの続き

(51) Int. Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｆ 7/08		Ｇ０７Ｆ 7/08	Ｊ
			Ｒ